OSG Summer Workshop Lubbock, 2011

Security

infrastructure, certificates and responsibilities

Anand Padmanabhan
for the OSG Security team

OSG Security model

A high level overview

OSG Security model

- Multiple administrative domains;
  each Site
  - Decides how to run its own resources
  - Decides which users to support
- Federated trust
  - Too many users and too many sites to require each user to register at each site
  - Virtual Organizations (VOs) as a middle man
    - A VO trusts its own users
    - A Site trusts a VO

Authentication structure

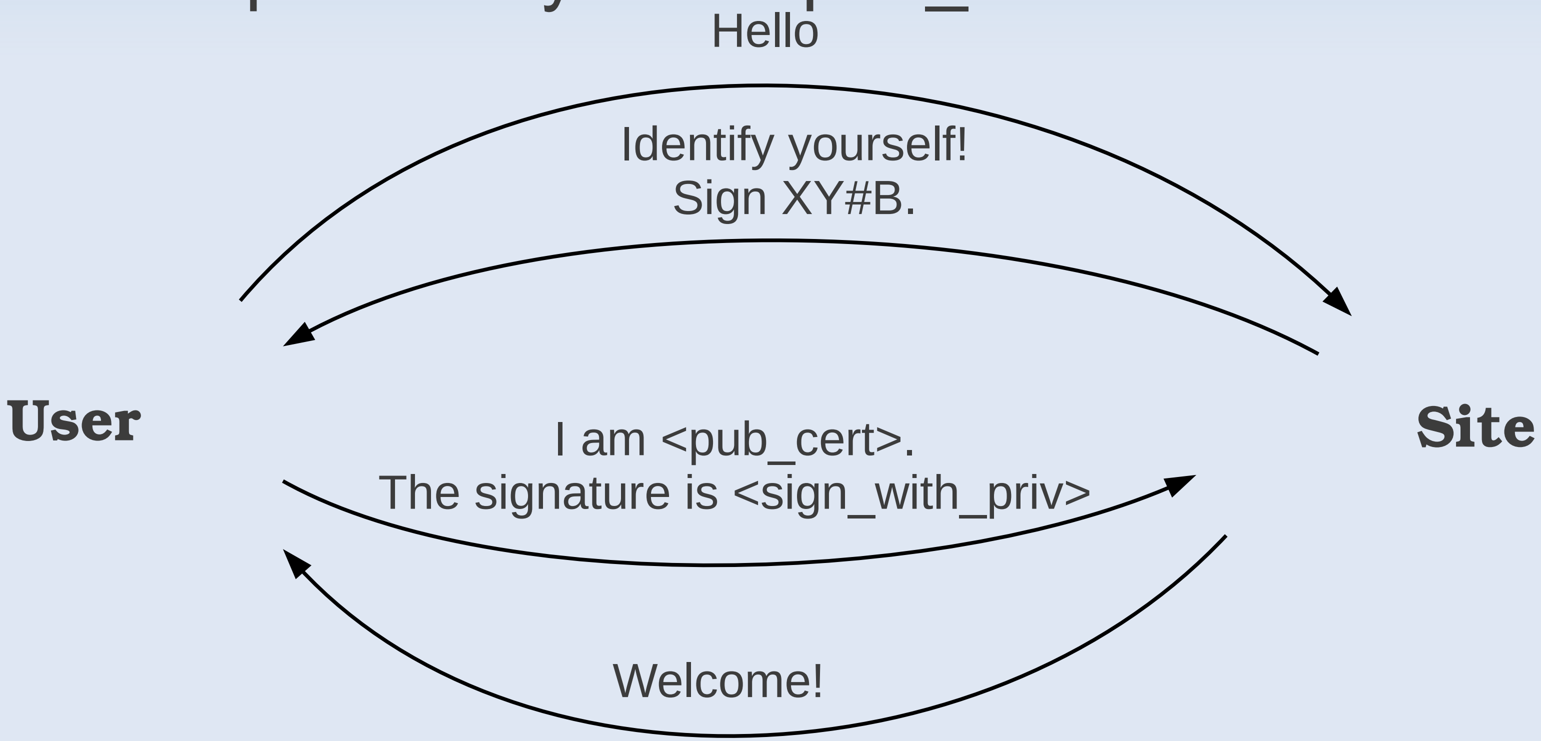
- Users want a single sign-on to run on all sites
  - Remember, they are not registering with all the sites
- Username+password cannot be used
  - That would require all sites to synchronize the password/shadow files -> not practical
- Public Key Infrastructure (PKI) used instead
  - In particular X.509 certificates and proxies
  - Sites only need to know the “user name”
    - PKI takes care of the security aspect

PKI – x.509 certificate

- The user is issued a certificate, which is composed of 2 parts:
  - A public part, containing
    - The user name (also known as the **DN**)
    - Validity period
    - The public key
    - The signing chain (more on this later)
  - A private part (containing the private key)
- **The private part MUST be kept private**
  - The public part can (and will) be sent around

PKI – How it works?

- User proves who he is
  by signing using the private key
  - The public key in the pub_cert allows for verification



PKI – What is a CA?

Not all CAs
are trusted!

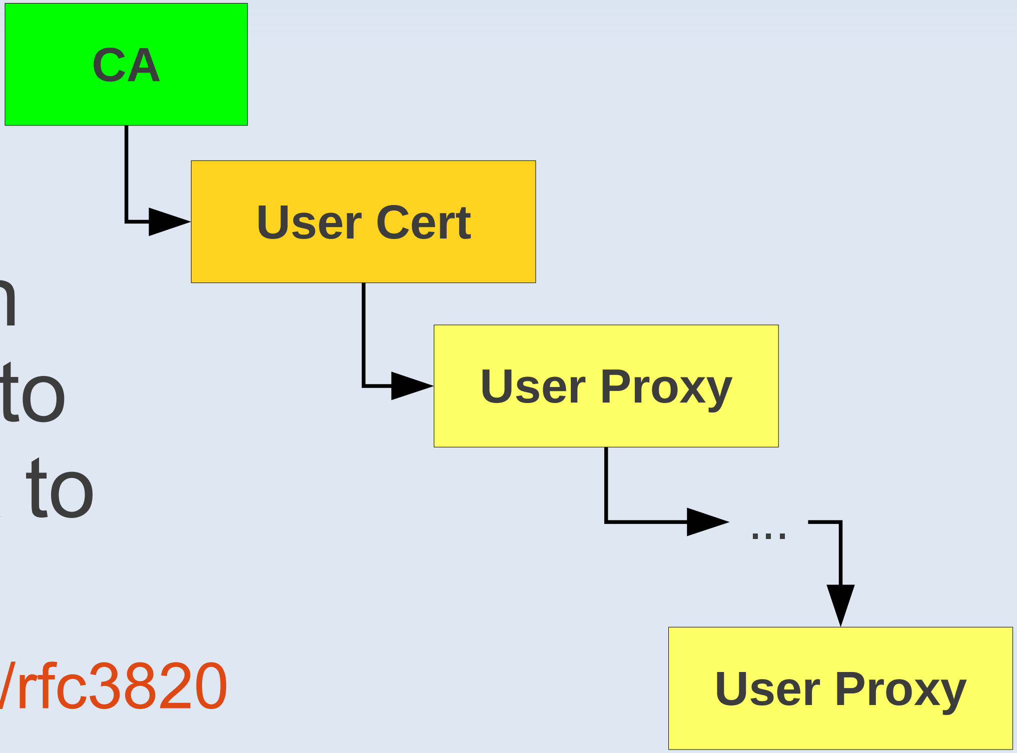
- A CA is someone who issues certificates
- A **trusted** CA is someone who you trust to issue user certificates **only if** they know that user
    - i.e. User **X** cannot get a certificate with username **Y**
- There are relatively few **trusted** CAs in existence
    - At least compared to the number of users
    - Pre-installing their public keys is thus manageable
- A CA can also revoke a user certificate
    - By publishing its public key in
      a Certificate Revocation List (CRL)
    - Make sure you download the updated CRLs often!

Self signed certs
not issued
by a trusted CA

PKI – And what is a proxy?

- You probably have heard about proxies
- A proxy is just a new certificate derived from a user certificate
  - Possibly many times!
- The signing chain contains the info to safely climb back to the CA

http://tools.ietf.org/html/rfc3820



PKI – Why a proxy?

- The user jobs may need to talk to a remote service when running on the worker nodes
  - But cannot access the user cert's private key!
- A proxy is thus sent (delegated) with the job to the worker node
  - **And the proxy contains a private key!**
  - So the job can impersonate the user
- Of course, delegating a private key is dangerous
  - Mitigated by the fact that proxy lifetime is short (much shorter than the user certificate one)

PKI – Sites have certificates, too

- Security only if mutual authentication
  - The Site trusts the User and
    the User trusts the Site
- The Site must prove who he is to the User
  - Especially if a proxy is being delegated there!
- All nodes with services at a Site thus need a host or service certificate
  - Similar to a user certificate, but issued by a CA for a specific DNS host
    (can only be used on that DNS address)

Authorization

- Just because someone can authenticate, does not mean a Site will authorize him/her to run on its resources
  - Authorization is a separate step
- The Site may also want to give different privileges to different users
  - The user must be mapped to a local security domain
  - Certificate DN -> (typically) UNIX UID

VO-based Authorization

- As mentioned in the introduction,
  Sites trust VOs (not users directly)
  - Each VO will keep a list of trusted user DNs
  - Through a service called **VOMS**
- OSG provides a list of trusted VOs and their VOMS servers
  - The Site needs to pick which VOs to support
  - Should always support the MIS VO (OSG operations)
- Users authenticate with a VOMS-extended proxy
  (voms-proxy-init -voms ...)

Mapping

- OSG provides **GUMS** for mapping
  - Talks to VOMS servers to get the list of user DNs
- Site admin must decide the mapping
  - Still VO based, possibly based on VO groups
  - Either pool **(recommended)** or group mappings
- The admin must also create all the necessary UNIX accounts
  - Part of *“administrative autonomy”* principle

OSG Security

Getting a Certificate

Which CAs do we use

- DOEGrids CA
  - https://pki1.doegrids.org/ca/
- CERN CA (Used by WLCG)
  - https://ca.cern.ch/ca/
- Fermilab CA (Fermilab-based users)
  - Converts krb5 tickets into certificates
- CAs accredited by IGTF (International Grid Trust Federation)
  - Many country typically have their own CA

CAs supported as a OSG site

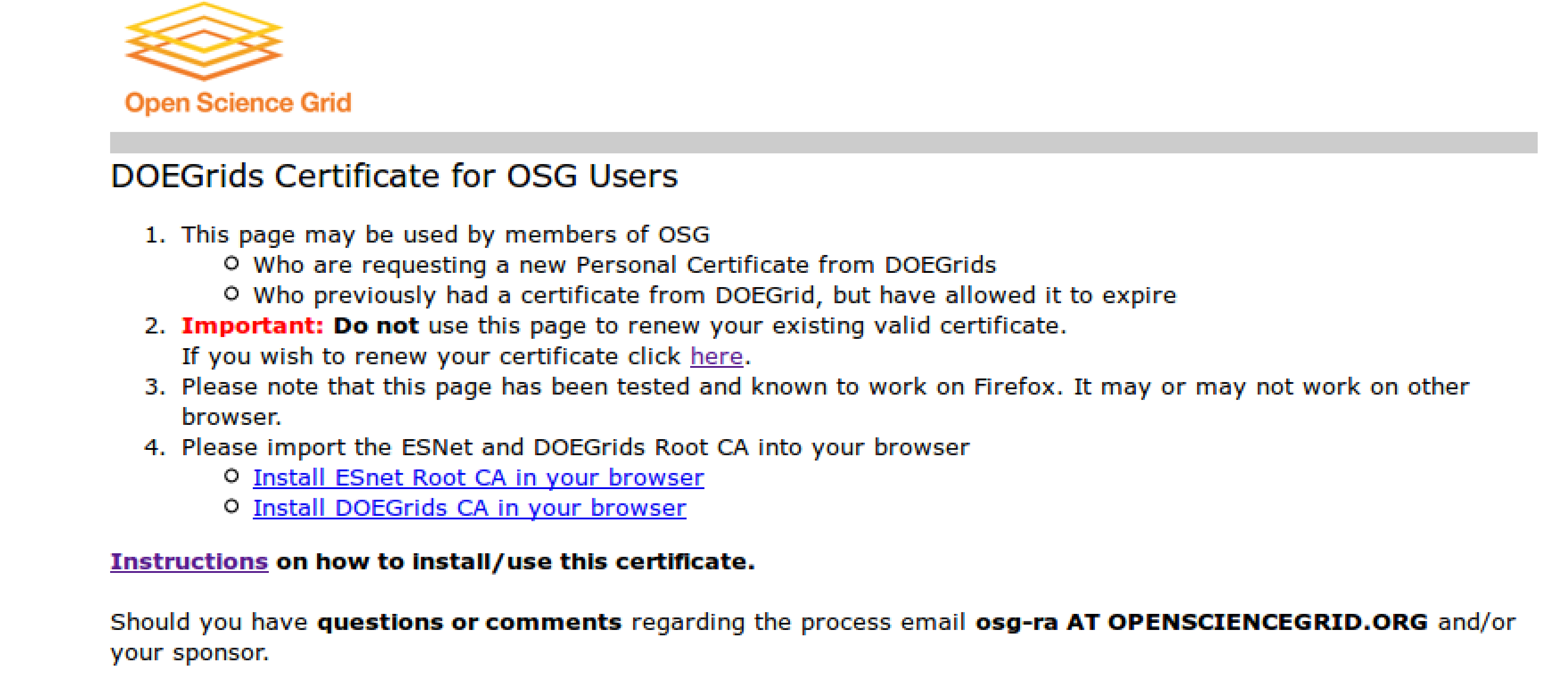
- OSG provides a list of trusted CAs known to be used by OSG-affiliated VOs
  - Get them trough VDT
    http://software.grid.iu.edu/pacman/cadist/ca-certs-version
- Sites choose which CAs to support
  - Typically most sites support OSG provided CAs
  - However they are free to add/remove CAs

Requesting a certificate

- Most likely you want to use DOEGrids
- You can request them either
  trough the Web interface or
  https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/CertificateGetWeb
  trough the command line interface
  https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/CertificateGetCmd
  - Command line easier for bulk requests
    (e.g. for service certificates)

Obtaining a personal certificate via browser

- https://software.grid.iu.edu/cert/certreg.php



Open Science Grid

DOEGrids Certificate for OSG Users

1. This page may be used by members of OSG
   - Who are requesting a new Personal Certificate from DOEGrids
   - Who previously had a certificate from DOEGrid, but have allowed it to expire
2. **Important: Do not** use this page to renew your existing valid certificate.
   If you wish to renew your certificate click here.
3. Please note that this page has been tested and known to work on Firefox. It may or may not work on other browser.
4. Please import the ESNet and DOEGrids Root CA into your browser
   - Install ESnet Root CA in your browser
   - Install DOEGrids CA in your browser

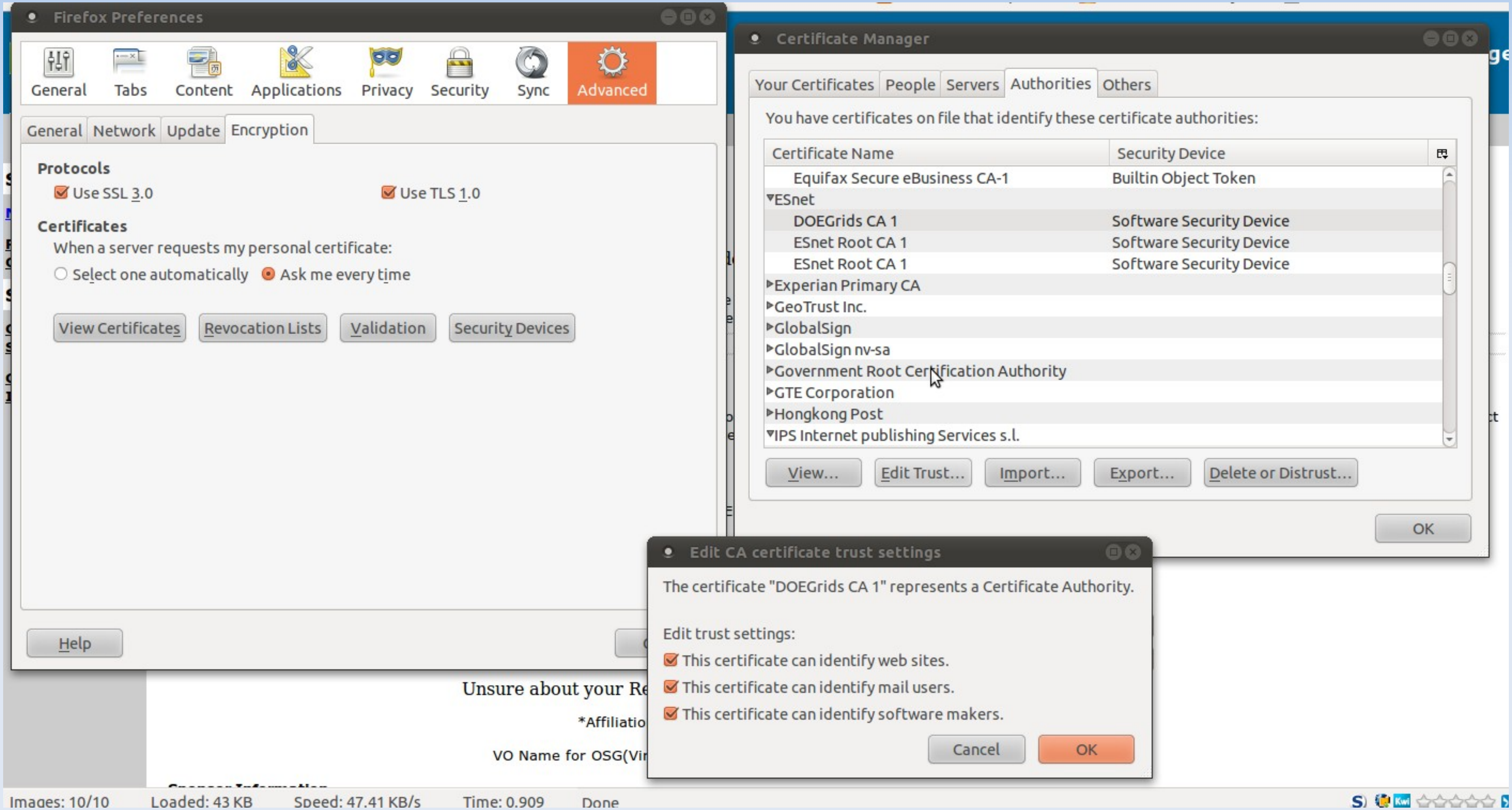
Instructions on how to install/use this certificate.

Should you have **questions or comments** regarding the process email **osg-ra AT OPENSCIENCEGRID.ORG** and/or your sponsor.

Installing root CA in browser

- Go to TACAR (TERENA Academic Certification Authority Repository)
  - https://www.tacar.org/
  - Certificates tab
  - Click install on which ever CAs you wish to install in your browser
    - Some browser keep browser specific CA repository (e.g. Firefox) while others rely on system wide repository
- By installing a CA you are asking your browser to trust the certificates issued by that CA

Locating root CA in your browser



Protocols

☑ Use SSL 3.0 ☑ Use TLS 1.0

Certificates

When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
Equifax Secure eBusiness CA-1	Builtin Object Token
▾ESnet	
DOEGrids CA 1	Software Security Device
ESnet Root CA 1	Software Security Device
ESnet Root CA 1	Software Security Device
▸Experian Primary CA	
▸GeoTrust Inc.	
▸GlobalSign	
▸GlobalSign nv-sa	
▸Government Root Certification Authority	
▸GTE Corporation	
▸Hongkong Post	
▾IPS Internet publishing Services s.l.	

The certificate "DOEGrids CA 1" represents a Certificate Authority.

Edit trust settings:

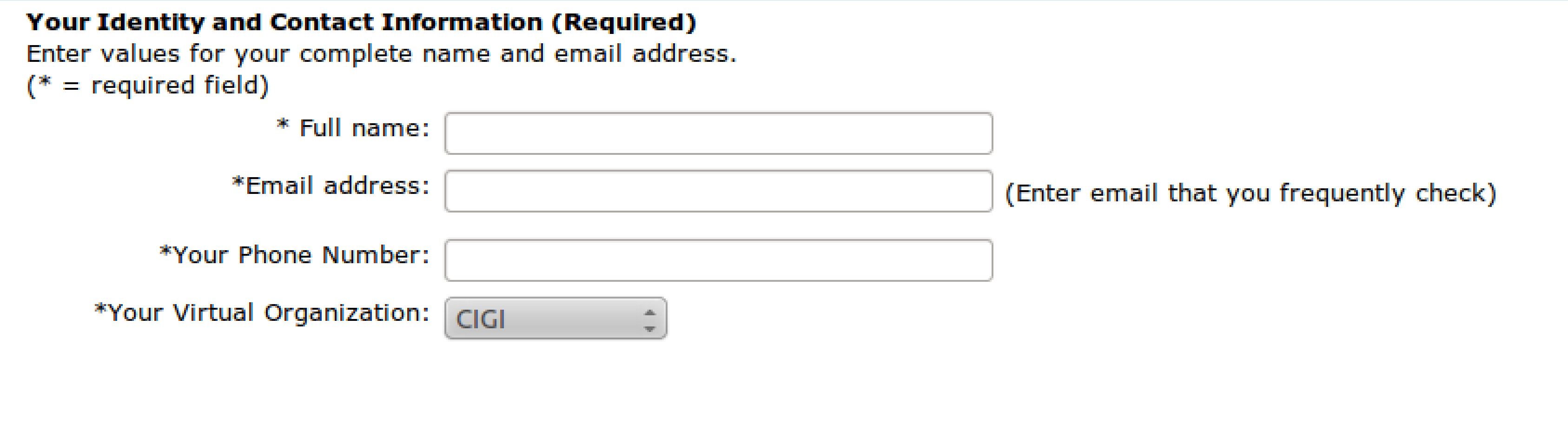
☑ This certificate can identify web sites.

☑ This certificate can identify mail users.

☑ This certificate can identify software makers.

Applying for a personal certificate

- Identity and Contact Information



Your Identity and Contact Information (Required)

Enter values for your complete name and email address.

(* = required field)

* Full name:

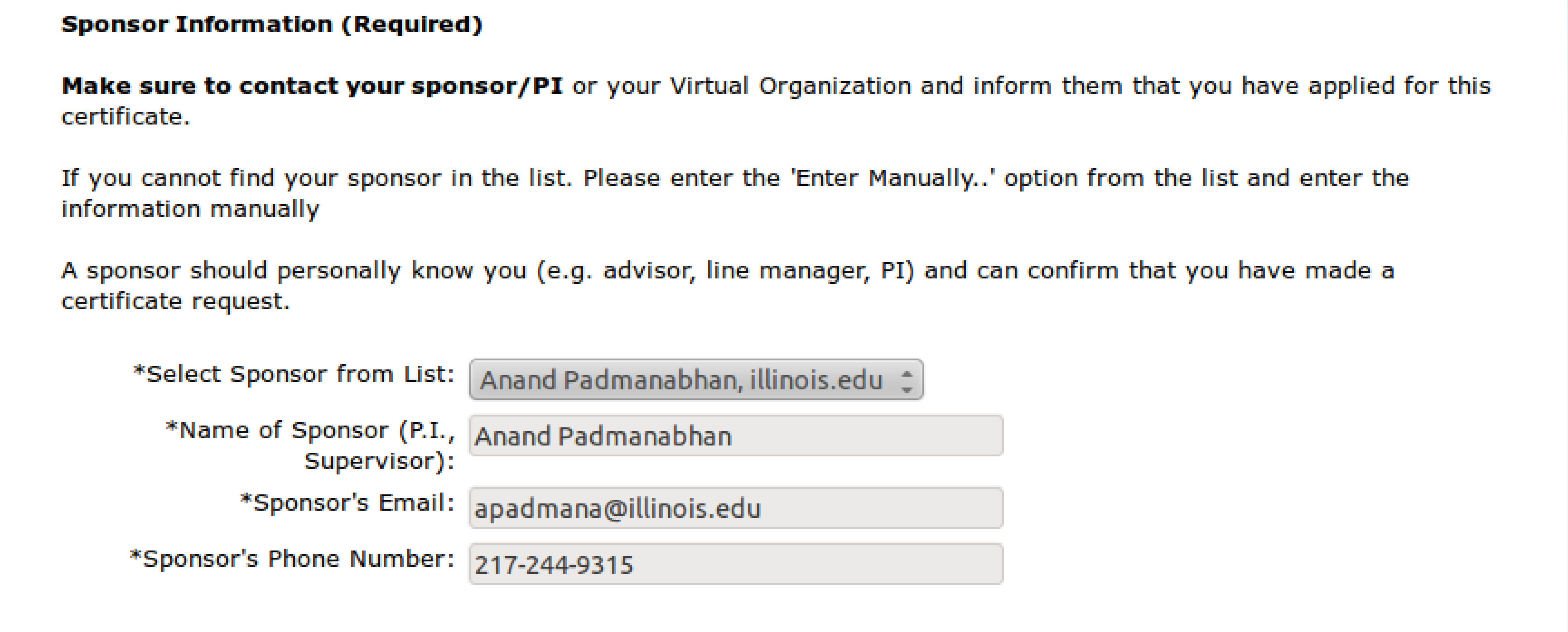
*Email address: (Enter email that you frequently check)

*Your Phone Number:

*Your Virtual Organization: CIGI

Applying for a personal certificate

- Sponsor Information



Sponsor Information (Required)

Make sure to contact your sponsor/PI or your Virtual Organization and inform them that you have applied for this certificate.

If you cannot find your sponsor in the list. Please enter the 'Enter Manually..' option from the list and enter the information manually

A sponsor should personally know you (e.g. advisor, line manager, PI) and can confirm that you have made a certificate request.

*Select Sponsor from List:	Anand Padmanabhan, illinois.edu
*Name of Sponsor (P.I., Supervisor):	Anand Padmanabhan
*Sponsor's Email:	apadmana@illinois.edu
*Sponsor's Phone Number:	217-244-9315

What happens next

- Your request goes to the OSG RA and is directed to appropriate RA agents
  - RA agents are typically VO representatives
- RA agent will contact the sponsor
  - Sponsor has to validate your request and identity
  - **This means that sponsor needs to know before hand you are requesting a certificate**
- Getting a certificate can take days. So apply early

What happens next

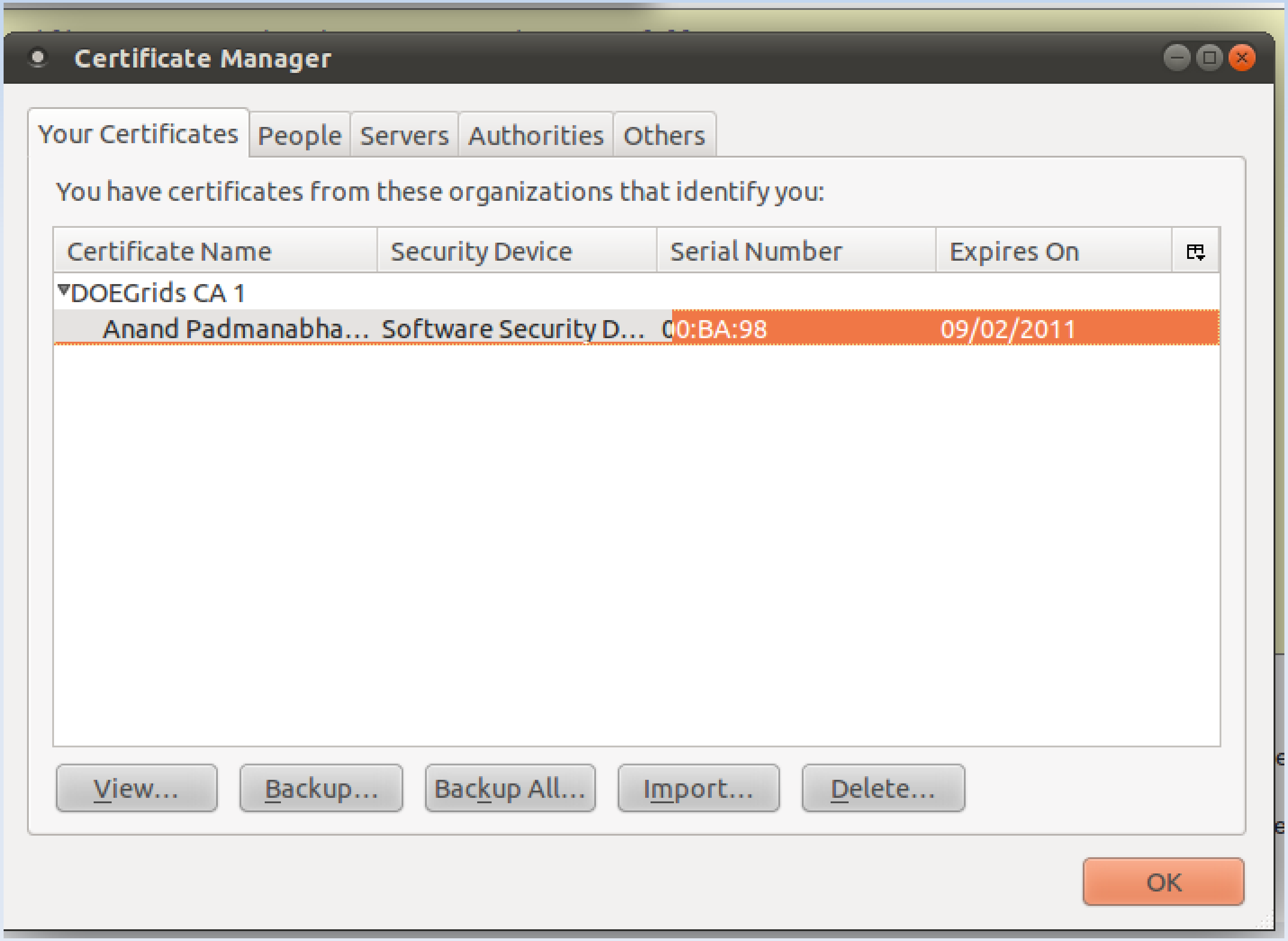
- Once the certificate is issued you will receive an email from CA with instructions on how to download the certificate
- NOTE: Your have to use the same browser & machine to retrieve the certificate that you used to submit the request.

Getting into a VO

- To use the OSG you need to be a member of a VO
- Typically your user certificate needs to be registered into VO VOMS server
  - Indicates membership in the VO and affords you access to resources available to that VO
- Registration procedure is VO specific
  - Please contact your VO

Exporting your certificate from browser

- Demo On Firefox



Certificate Manager

You have certificates from these organizations that identify you:

Certificate Name	Security Device	Serial Number	Expires On
▾DOEGrids CA 1			
Anand Padmanabha…	Software Security D…	00:BA:98	09/02/2011

Certificate format

- Two formats
  - .p12–single file, contains both public and private part
  - .pem–two files, one for public (cert.pem) and one for private part (key.pem)
- .p12 and key.pem must be private to the user
  - No group or world read permissions!
- Can convert between them

```
openssl pkcs12 -clcerts -nokeys -in cert.p12 -out usercert.pem
openssl pkcs12 -nocerts -in cert.p12 -out userkey.pem
openssl pkcs12 -export -in cert.pem -inkey key.pem -out cred.p12
```

Renewing certificate

- Renew your certificate before they expire
  - You can keep the same DN
  - You do not have to go through the approval process again
- Use: https://software.grid.iu.edu/cert/certrenew.php
-

OSG Security

Security responsibilities

What is security?

- Security is much more than just technology
  - It is as much a social problem
  - Keep your contact information up-to-date in OIM
- We have a secure system only if the participants act responsibly
- Malicious participants are obviously removed from the system
  - But a careless one can make almost as much damage!
- Know your responsibilities

Protect your grid credential

- Store your private key only in secure locations
  - Store it only in a file that is accessible to yourself alone
  - Set unix permission as 400 (owner readable only)
- Do not keep unnecessary copies
- Do not copy it to or store it in a directory that is accessible to the network.
- Private key should be encrypted with a complex passphrase known only to you
  - Sharing your key is a immediate ground for its revocation
- You may keep your certificate and private key in browser, but keep it encrypted using browser features (e.g. master password)

Abide by you VO policies

- Every VO through which you access OSG resources has a science mission for which use of these resources is allowed
- Use of OSG resources in a manner that is not directly or indirectly meeting the purpose of your VO, then you are in violation of the OSG acceptable use policy (AUP)
- Your VO may suspend your access to OSG
- Familiarize yourself with OSG user AUP
    - http://osg-docdb.opensciencegrid.org/cgi-bin/ShowDocument?docid=86

What if your certificate is suspected of being compromise

- If you suspect a compromise, immediately notify the OSG security team https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/IncidentDiscoveryReporting
    - Even if it turns out that it was a false alarm, better safe than sorry
- Notify the CA and have them revoke your certificate
- If you suspect or have knowledge of a security incident, please report it immediately to your VO security contact and the OSG security team
    - For e.g, if your campus folks tell you your machine was infected

Communicating with security team

- Learn to securely communicate with security team
- Security announcement sent by OSG security team are signed using the security teams PGP key
  - Please read all security announcements
  - Learn how to verify signatures
  - PGP clients are available for popular email clients
  - https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/SecureEmail
- You can also send an encrypted email to security team or any of its team members
  - https://twiki.grid.iu.edu/bin/view/Security/SecurityTeamMembers

Summary

- Security is both a social and technical problem
- Certificates are used for authentication, authorization is a separate step
  - Keep your private part of certificate private
  - Do not share your certificate or passwords
- Keep your contact information up-to-date in OIM
- Know how to request and renew cetificates
- Report security incidents immediately

Additional readings

- OSG Security Home page
  https://twiki.grid.iu.edu/twiki/bin/view/Security/
- OSG Certificate page
  https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/CertificateWhatIs
- OSG Security and Certificates FAQ
  https://twiki.grid.iu.edu/bin/view/Documentation/OsgFaq#Security_and_Certificates
- OSG Certificate Request Documentation
  https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/CertificateGet
- OSG User Security Responsibilities
  https://twiki.grid.iu.edu/bin/view/ReleaseDocumentation/SecurityUserResponsibilities
- NCSA OpenSSL Cheatbook
  http://security.ncsa.illinois.edu/research/grid-howtos/usefulopenssl.html

Thank YOU!